UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 5 | Issue 1 Article 6

2001

Financial Services Privacy at the Start of the 21st Century: A Conceptual Perspective

Charles M. Horn

FINANCIAL SERVICES PRIVACY AT THE START OF THE 21ST CENTURY: A CONCEPTUAL PERSPECTIVE

CHARLES M. HORN*

I. INTRODUCTION

The enactment of the Gramm-Leach-Bliley Act (GLBA)[1] was, for many reasons, a seminal event in the financial services markets. Not only did GLBA usher in a new era of financial services deregulation and competition, but it also reconfigured, in important respects, the regulatory landscape for financial services in the United States. For example, GLBA created a broad federal legislative and regulatory framework for the protection of personal financial information collected by financial institutions, requiring financial institutions to tell their customers what personal information they are collecting and how it is being used. Financial institutions are also required to give consumers a choice as to whether their personal information may be shared with others.[2]

GLBA's financial privacy requirements will become fully effective with the implementation of uniform regulations adopted by the financial institutions regulatory agencies[3] in July 2001.[4]

---

* Charles M. Horn is a partner with the Washington, DC office of Mayer, Brown & Platt, where he specializes in financial services regulatory and transactional matters. Mr. Horn received his J.D. in 1976 from Cornell Law School and is a member of the District of Columbia bar. The author gratefully acknowledges the research and editorial assistance of Cathleen M. Tefft in the preparation of this article.

1. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections predominantly of 12 and 15 U.S.C.).

2. Gramm-Leach-Bliley Act § 501-10; 15 U.S.C. §§ 6801-6810, 6821-6827 (Supp. V 1999).

3. The financial institutions regulatory agencies include the five federal financial institutions regulatory agencies—the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Federal Reserve Board or FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA)—the Securities and Exchange Commission (SEC), and the Federal Trade Commission

Most financial institutions have taken substantial measures to bring themselves into compliance with what promises (or threatens) to be a complex and challenging financial regulatory scheme, although the continued development and refinement of this scheme undoubtedly will continue for months and years to come. At the same time, the principles embodied in this new scheme are relatively straightforward and reflect a general public concern over the collection by commercial entities of personal information of all kinds.

The intent of this article is to convey a conceptual understanding of these principles and concerns that will assist financial services providers and others in appreciating the context and application of these new privacy requirements. At the same time, the privacy requirements of GLBA and the implementing federal regulations are complex in their application, and a microcosmic review of these requirements and their implications is beyond the scope of this discussion.

II. BACKGROUND

The right to privacy, sometimes referred to as the "right to be left alone," has become an integral and increasingly important part of the United States cultural and legal landscape.[5] Americans,

---

(FTC).

4. Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40 for the OCC; 12 C.F.R. pt. 216 for the Federal Reserve Board; 12 C.F.R. pt. 332 for the FDIC; and 12 C.F.R. pt. 573 for the OTS); Privacy of Consumer Financial Information, 65 Fed. Reg. 31,740 (May 18, 2000) (to be codified at 12 C.F.R. pt. 716 for the NCUA); Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,334, 40,362 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248 for the SEC); Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313 for the FTC).

5. Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *See also* Warden v. Hayden, 387 U.S. 294, 310-12 (1967) (Fortas, J., concurring); *Id. at* 310-12 (Douglas, J., dissenting) (quoting N. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION (1937)); Stanford v. Texas, 379 U.S. 476, 482 (1965); Boyd v. United States, 116 U.S. 616, 630 (1886); DAVID H. FLAHER, PRIVACY IN COLONIAL NEW ENGLAND (1972); Shirley M. HUFSTEDLER, THE DIRECTIONS AND MIS-DIRECTIONS OF A CONSTITUTIONAL RIGHT OF PRIVACY, 546 (1971); JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT (1966); ROBERT A. RUTLAND, THE BIRTH OF THE BILL OF RIGHTS (1955). The case of *Entick v. Carrington*, which

by and large, expect that they should be able to conduct their personal or business affairs beyond the prying eyes of others, and the ability to do so has become one of the cherished freedoms of contemporary American life. However, this "right" increasingly is being threatened by the growth of government functions and services, and the increasing dependency of individuals on technology in all aspects of their personal and commercial lives, both of which have resulted in the generation of enormous amounts of highly detailed and revealing personal information that is all-too-readily accessible by others. Most recently, the growth of the Internet has generated increased levels of public and legislative anxiety over the privacy of personal information, and the ability of individuals, if they so choose, to protect the confidentiality of that information.

The right to privacy comes in various colors and hues: the general right to conduct one's personal affairs (including interpersonal and sexual) in private; the right to be protected from unreasonable searches by police authorities; and the right to have one's personal information used properly by the government and others. Each of these manifestations of personal privacy has been the subject of extensive public discussion, and ultimately legislative and judicial protections of various kinds. Indeed, in several of its manifestations, the right to privacy has been given a certain level of Constitutional protection.[6] Yet, in many respects the legal protections afforded to the privacy rights of individuals have tended to lag by some period of time the misuses and abuses of these rights.

Such is the case with personal financial privacy, which refers to the right of an individual to control the collection, disclosure and use of personal information concerning his or her financial transactions and affairs. Concerns over the collection and use of personal information by the government and private

---

outlawed general warrants, is generally viewed as the wellspring of the Fourth Amendment. *Boyd*, 116 U.S. at 616, 626-27 (citing Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765)); *Stanford*, 379 U.S. at 484. The First Amendment right to association has also been viewed as providing a right privacy, but not in the context of bank records. *See, e.g.*, Louisiana ex rel. Gremillion v. NAACP, 366 U.S. 293 (1961); NAACP v. Alabama, 357 U.S. 449 (1958).

6. *See* Brandeis & Warren, *supra* note 5.

parties alike are not new. In 1973, the U.S. Department of Health, Education and Welfare published a report titled *Records, Computers and the Rights of Citizens*, in which the Department articulated what. by all accounts. was the first in a series of "fair information collection principles."[7] In the next quarter century, a variety of governmental bodies periodically examined the issues associated with the collection and use of personal information and attempted to establish bodies of principles or "best practices" regarding such collections and uses.[8]

In turn, during the 1970's and 1980's, federal legislation was enacted to restrict the ability of the government to access personal financial information in the hands of financial institutions,[9] to limit the uses and disclosures by creditors of personal financial information provided to them by their customers,[10] and to address a variety of other specific acts and practices.[11] And, although the

7. RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (July 1973), http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited Feb. 21, 2001).

8. *See, e.g.*, THE PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977); ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, ORGANIZATION FOR CO-OPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org//dsti/sti/it/secur/prod (last updated Jan. 5, 1999); PRIVACY WORKING GROUP, INFO. POLICY COMM., INFO. INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995), *available at* http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html (last visited Feb. 28, 2001); U.S. DEPT. OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), *available at* http://www.ntia.doc.gov/ntiahome/privwhitepaper.html (last visited Feb. 28, 2001); Council Directive 95/46/EC, 1995 O.J. (l 284) 31-50; CANADIAN STANDARDS ASSOCIATION, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION: A NATIONAL STANDARD OF CANADA (1996), *available at* http://www.csa.ca/english/home/index.htm (last visited Feb. 23, 2001).

9. The Right to Financial Privacy Act of 1974, which was adopted in response to the Supreme Court's decision in *U.S. v. Miller*, 425 U.S. 435 (1976), held that financial institution customers have no rights to protection from government access of personal financial information obtained from a financial institution. 12 U.S.C. §§ 3401-21 (1994).

10. *See* The Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. §§ 1681a-t (Supp. IV 1998). The FCRA places restrictions on the right of a creditor to disclose to third parties credit information without the consent of the consumer affected, other than information concerning the transactions of that consumer ("transaction" or "experience" information) with that creditor. 15 U.S.C. § 1681m (Supp. IV 1998).

11. *See* L. Richard Fischer, *Privacy and Accuracy of Personal Information*, 3 N.C.

protections afforded by these various federal laws were substantial, the legislatures and the courts, by and large, did not develop any comprehensive, systematic or coherent scheme of legal protections for personal financial information during that period.

As the age of online technology shifted into high gear in the 1990's, however, various administrative bodies stepped into the breach to fashion a variety of guidelines and legal remedies to address a perceived misuse of personal financial information by commercial enterprises. As a general matter, these actions were premised on the *misuse* of personal information in a *deceptive and misleading* fashion, a course of conduct which gave rise to remedial actions under state consumer protection laws.[12] They were not, nor could they be, premised on any affirmative personal right to privacy in one's financial affairs, because no such comprehensive right existed. Moreover, while the FTC took action against various online commercial enterprises for misuse of consumer information, it generally lacked the authority under the FTC Act to take action against financial institutions for such conduct.[13]

As time passed, privacy protection issues gradually began moving onto the center stage of the legislative and regulatory arena, undoubtedly helping to create a more favorable environment for the enactment of financial privacy protections. For example, in the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[14] Congress specifically

---

BANKING INST. 11, 14 (1999).

12. *See* Hatch v. U.S. Bank Nat'l Assoc., et al., No. 0:99cv872 (D. Minn. filed June 9, 1999), *available at* http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_06091999.html (last visited Mar. 1, 2001); *In the Matter of The Chase Manhattan Bank* (Assurance of Discontinuance, Attorney General of the State of New York, 1999) (press release *at* http://www.oag.state.ny.us/press/2000/jan/ jan25b_00.html (last visited Mar. 1, 2001)). Both actions were taken by state authorities against banks which, according to the state authorities, shared personal financial data with third parties (telemarketers) without disclosure to, or the consent of, affected bank customers, thereby violating state consumer protection laws.

13. *See infra* note 27. Although section 18(f) of the FTC Act prohibits unfair and deceptive practices by banks, the FTC does not have the authority to take action against financial institutions for such activities; that authority instead is vested in the various federal financial institutions regulatory agencies. 15 U.S.C. § 57a(f) (1994).

14. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, § 264, 110 Stat. 1936.

directed the Department of Health and Human Services (HHS) to adopt regulations providing for the protection from disclosure of personal medical records and information without the affirmative consent of the affected individual. HIPPA thus required disclosure to individuals of how medical information would be collected, used and disclosed.[15] Shortly thereafter, Congress passed the Children's Online Privacy Protection Act of 1998 (COPPA)[16] in response to general public concerns over the collection and use by Internet service providers of children's personal information. This law created new obligations for online service providers that offered "kids' sites," which the operators knew were being accessed by children, to make disclosures to children *and their parents* concerning the collection and uses of children's online personal information. COPPA required online services to obtain "verifiable parental consent" prior to the collection and use of such information, and directed the FTC to adopt implementing regulations.[17]

Similarly, developments overseas generated additional attention with respect to privacy issues. Most notably was the European Commission's 1995 Directive on the Protection of Personal Data,[18] which has potential negative implications for the ability of European Union (EU) data collectors to share personal data with parties in the United States. Put simply, the EU Directive required EU member states to adopt legislation providing for the protection of personal data, and restricted the sharing of such data with persons in non-EU states that were found to have inadequate privacy protections for personal data. The United States, in the view of the EU, was one such noncompliant state. The potential impact of the EU Directive on transborder transfers of personal information generated a series of

15. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164). The HHS rules became effective on February 26, 2001.

16. 15 U.S.C. §§ 6501-6505 (Supp. IV 1998). COPPA became effective on April 21, 2000. *Id.*

17. 16 C.F.R. pt. 312.1-.12 (2000). Final FTC regulations were adopted in November 1999, effective April 21, 2000.

18. Council Directive 95/46/EC, 1995 O.J. (L 284) 31-50. The Directive became effective on October 25, 1998. *Id.*

discussions between the United States, through the Department of Commerce, and the EU, which resulted in the implementation of "Safe Harbor Privacy Principles" in July 2000. The Principles created a "safe harbor" from the applicability of the EU Directive for United States commercial enterprises that received personal data from the EU and complied with the various fair information conditions set forth in these Principles.[19]

Indeed, the increasing interest of governmental authorities, including the FTC, in privacy issues arising from heightened concerns over the collection and use of personal information online, was a substantial catalyst for increased legislative action. For example, the U.S. Department of Commerce was active in the study of privacy issues, both in response to the EU Directive and as part of a more generalized Clinton Administration concern over personal privacy, with a particular emphasis on privacy issues in electronic commerce and whether regulation, as opposed to industry self-regulation, was needed.[20]

Further, as early as 1995, the FTC staff began public inquiries into online privacy practices and concerns. Subsequent workshops, staff reports, and hearings[21] led ultimately to the publication in June 1998 of *Privacy Online: A Report to Congress*,[22] in which the FTC reported on the results of its wide-ranging surveys into online personal information collection practices of commercial service providers. The FTC expressed its concerns that most commercial web sites failed to provide basic privacy protections to consumers, and, perhaps more significantly, that

19. Notice of Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (Jul. 24, 2000). While the Safe Harbor Privacy Principles do not extend to entities that are not under the jurisdiction of the FTC or the Department of Transportation, including U.S. financial institutions, by political agreement between the U.S. and the EU, the EU Directive will not be applied, for the interim period, to personal data transfers to financial institutions subject to the GLBA privacy regulatory scheme, pending the EU's assessment of the efficacy of the U.S. implementation efforts under GLBA.

20. *See* Fischer, *supra* note 11, at 21-25.

21. The results of many of these inquiries are reported in an FTC staff report. FEDERAL TRADE COMM., PUB. WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFO. INFRASTRUCTURE (Dec. 1996), http://www.ftc.gov/reports/privacy/privacy1.htm (last visited Feb. 21, 2001).

22. *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* http://www.ftc.gov/reports/privacy3/index.htm (last visited Feb. 21, 2001).

existing industry efforts at self-regulation had been of limited success.[23] The FTC recommended legislative action to create online privacy protections for children (an area of more immediate and acute concern to the FTC) – a recommendation which led directly to the passage that same year of COPPA – and stated that it would subsequently recommend an "appropriate response" to protect the online privacy of all consumers.[24] The FTC Report also articulated what were described as five "Fair Information Practice Principles:" (i) *notice/awareness* of an entity's information practices; (ii) *choice/consent* as to how personal information can be used; (iii) *access/participation* allowing consumer access to personal data and the opportunity to correct it; (iv) *integrity/security* of personal data; and (v) *enforcement/redress* of consumer privacy protections.[25] These principles, in various manifestations, would become part of the legislative model for personal financial privacy discussed below. Subsequently, in the summer of 2000, the FTC concluded that a legislative response to create online privacy protections for consumers was needed.[26] In addition, the FTC instituted various actions in response to alleged deceptive and misleading collections and uses of personal information by online merchants and service providers in violation of section five of the Federal Trade Commission Act (FTC Act).[27]

---

23. *Id.*

24. *Id.*

25. *Id.*

26. FED. TRADE COMM'N, DIVISION OF FINANCIAL PRACTICES, BUREAU OF CONSUMER PROTECTION, PRIVACY ONLINE: FAIR INFORMATION COLLECTION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS iii (May 22, 2000), *available at* http://www.ftc.gov/os/2000/05/index.htm#22 (last updated Oct. 3, 2000). The FTC, noting that online privacy continued to present "an enormous public policy challenge," said that online privacy legislation was needed, although it commended the online industry for its self-regulatory efforts with respect to personal privacy online. *Id.* at ii. The FTC articulated four basic fair information practice principles for a legislative framework: (1) notice; (2) choice; (3) access; and (4) security. *Id.* at 4. These were the same principles (less enforcement/redress) set forth in the FTC's 1998 report. *Id.* Interestingly, in a 1999 report to Congress on online privacy, the FTC expressed the view that legislation was "not appropriate" at the time, indicating that the FTC would work with industry groups and public sector participants to encourage the promotion of online fair information principles. FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS (July 1999), *available at* http://www.ftc.gov/os/1999/9907/index.htm#13 (last visited Mar. 1, 2001).

27. 15 U.S.C. § 45(a) (1994). *See, e.g., In re* Geocities, Inc., Trade Reg. Rep.

III. THE ENACTMENT OF FEDERAL FINANCIAL PRIVACY LEGISLATION

Notwithstanding the distinct "online" orientation of the FTC in its privacy initiatives, the FTC's concerns over privacy, and the concerns of other governmental authorities, carried over more generally into the financial services industry. Congress began to examine with greater interest the need for a legislative framework at the federal level to create increased privacy protections for individuals doing business with banks, securities firms, insurance companies and other classes of financial institutions. The financial services industry, wary of the possibility of a new and intrusive scheme of federal legislation and regulation, urged legislative restraint, arguing instead for the adoption of voluntary self-regulatory measures. At the same time, federal regulators issued a variety of supervisory pronouncements addressing the issue of financial privacy protections for consumers,[28] and warned the industry that unless the industry took affirmative action to confer greater privacy protections on their customers, a federal legislative solution would be difficult to avoid. In addition, reports of widespread instances of identity theft, through acts such as "pretext calling" (the practice of deceiving banks and bank customers into revealing personal financial information under false pretenses), attracted the attention of federal regulators and their legislative overseers. These reports led various federal banking agencies to warn against such practices.[29] Perhaps more importantly, the reports simply added fuel to the growing concerns over the protection of personal financial information.

(CCH) ¶ 24-485 (1999); *In re* Liberty Fin. Co., Inc., Trade Reg. Rep. (CCH) ¶ 24-598 (1999); FTC v. ReverseAuction.com, Trade Reg. Rep. (CCH) ¶ 73-001 (D.D.C. 1999); FTC v. Rennert, Trade Reg. Rep. (CCH) ¶ 73-006 (D. Nev. 2000); FTC v. Toysmart.com., No. 00-11341-RGS (D. Mass. 2000) (stipulated consent agreement and final order), *available at* http://www.ftc.gov/os/2000/07/toysmartconsent.htm (last visited Mar. 1, 2001).

28. *See, e.g.*, FDIC, ONLINE PRIVACY OF CONSUMER PERSONAL INFORMATION (1998), *available at* http://www.fdic.gov/news/news/financial/1998/fil9886b.html (last visited Feb. 21, 2001); OTS, POLICY STATEMENT ON PRIVACY AND ACCURACY OF PERSONAL CUSTOMER INFORMATION (Nov. 1998), *available at* http://www.ots.treas.gov/docs/25097.pdf (last visited Mar. 1, 2001).

29. *See, e.g., Pretext Phone Calling*, OCC Advisory Letter 98-11 (Aug. 20, 1998), 1998 WL 549337.

By the same token, interest in financial privacy at the state level continued to wax. A number of states introduced financial privacy legislative measures,[30] and other states took action against financial firms that they believed were misusing personal customer information by selling it to telemarketers and other third parties.[31] Even though these various state legislative proposals generally did not lead to final state legislative action, these actions clearly signaled that the states intended to be part of the privacy debate—a point that was not lost on federal legislators and regulators.

Thus, although industry initiatives on privacy self-regulation continued, in the final analysis these efforts were not sufficient to forestall continued congressional interest and action with respect to financial privacy legislation, and legislative efforts on privacy continued into the 106th Congress during 1999. At the same time, Congress was also considering major financial reform legislation touching upon a number of key elements, including the expansion of bank powers, provisions allowing securities and insurance firms to enter the banking business (and vice versa), the realignment of federal regulatory jurisdiction among various federal "functional" regulators—namely, the elements that became the core of GLBA—and a variety of other matters. The momentum of financial reform led congressional leaders interested in financial privacy to use the former as the legislative vehicle for enactment of the latter, and in due course the principal financial reform bill then pending in the House, H.R. 10, was amended to add provisions specifically addressing consumer financial privacy.

These additions proved to be contentious. At the heart of the debate was the question of how, and to what extent, financial institutions would be able to share consumer financial information with their affiliates and third parties. Consumer groups and their congressional advocates urged that financial firms be required to obtain the affirmative consent of their customers prior to being allowed to share personal information with affiliates and third

30. *See, e.g.*, S. 252, 140th Gen. Assem., 1st Special Sess. (Del. 1999), WL 1999 DE S.B. 252 (SN); H.R. 4483, 181st Gen. Ct., Reg. Sess. (Mass. 1999), WL 1999 MA H.B. 4483 (SN); H.R. 5249, 182nd Gen. Ct., Reg. Sess. (Mass. 2000), WL 1999 MA H.B. 5249 (SN).

31. *See supra* note 27.

parties alike, a view that was shared by a number of state representatives. These requirements were vigorously opposed by the financial services industry, as well as influential congressional leaders, who argued that these types of financial privacy-based restrictions would significantly interfere with the cross-selling of new products and services and thus seriously dilute the legislation's cross-industry affiliation and new powers provisions. Accordingly, the industry argued that self-regulation should be given a chance to work. In fact, at several junctures the financial services industry indicated that it might be forced to oppose any legislation that required affirmative customer consent (customer "opt in"), or other restrictions on the sharing of customer information with affiliates.[32]

But, in the waning days of the fall of 1999, a series of last-minute compromises were reached among Senate and House leaders to modify the legislation's privacy provisions to (1) require financial institutions to disclose to their customers their policies and practices with regard to the collection, use, and disclosure of customer information (privacy policies), (2) permit financial firms to share customer information with affiliates without restriction, and (3) permit consumer information to be shared with third parties provided that the consumer, after receiving notice from the financial institution, had not directed that such information not be shared (or, put another way, the consumer had not "opted out" of such sharing).[33] Further, in deference to state interests, the legislative compromise allowed individual states to "trump" the federal privacy requirements by enacting more stringent privacy protections.[34] This late compromise allowed the legislation to

32. The major financial services trade associations sent a joint letter to key congressional leaders in October 1999 stating that "our associations will find it necessary to oppose any legislation ... [seeking] to impose 'opt-in' requirements and/or to impose new restrictions on the sharing of information among affiliates." Letter from the Securities Industry Association, American Bankers Association, American Council of Life Insurance, American Insurance Association, Financial Services Council, and Investment Company Institute to the Hon. Phil Gramm, U.S. Senate, and the Hon. James Leach and Richard Bliley, U.S. House of Representatives (Oct. 13, 1999), *available at* http://www.aba.com/press+Room/PR_Grammletter.htm (last visited Feb. 27, 2001).

33. *See infra* text accompanying notes 37–44.

34. *See infra* Part VI.B.2.

proceed forward to passage by both Houses of Congress and enactment into law by President Clinton on November 12, 1999. Nonetheless, proponents of stricter privacy requirements have promised that the debate is not over and that stricter privacy measures will be considered in the next session of Congress.

IV. PRIVACY REQUIREMENTS OF GRAMM-LEACH-BLILEY: THE FINANCIAL SERVICES MODEL

The financial privacy requirements of GLBA, set forth in Title V,[35] incorporate in substantial respects the basic "fair information" principles of notice, choice, and security enunciated by the FTC and other regulatory bodies, discussed above.[36] To a lesser extent, GLBA also incorporates the principles of access and redress, albeit in a less apparent manner. In reflecting these principles, however, GLBA, as well as the implementing federal regulations, makes several important choices in how these principles are applied. Indeed, these choices embody the legislative compromises that were made in the final weeks of the 106th Congress that allowed GLBA to become law.

The principal requirements of Title V are straightforward: (1) all financial institutions must provide their customers with initial and annual written privacy notices informing customers as to what nonpublic personal information is collected from them, how this information is maintained and used, and with what persons this information is shared;[37] and (2) financial institutions must give consumers from whom they obtain nonpublic personal information notice of the institution's intention to share such information with unaffiliated third parties, and an opportunity for the consumer to direct that the information not be shared (the right to "opt out").[38] However, Title V allows financial institutions to freely share nonpublic personal information with their affiliates.[39] Further, Title V permits financial institutions to share

35. Gramm-Leach-Bliley Act § 501-10; 15 U.S.C. §§ 6801-6810, 6821-6827 (Supp. V 1999).

36. *See supra* text accompanying note 25.

37. 15 U.S.C. § 6803 (Supp. V 1999).

38. 15 U.S.C. § 6802(b) (Supp. V 1999).

39. 15 U.S.C. § 6802(b)(2) (Supp. V 1999).

information with third parties without giving consumers notice and the right to opt out for a variety of specified purposes, including customer transaction processing and servicing, law enforcement purposes, security purposes as a part of a business combination, or with the consumer's consent.[40] Title V also allows financial institutions to share information with third parties for joint marketing purposes pursuant to the terms of a written agreement.[41] At the same time, however, the law imposes a broad prohibition on the transfer of customer account identifiers to third parties for marketing purposes.[42] Title V, in turn, directs the federal financial institution regulatory agencies (the banking agencies, SEC and FTC) to adopt regulations implementing these requirements.[43] Entities regulated by the Commodity Futures Trading Commission, however, as well as certain secondary market financial intermediaries, were expressly excluded from the coverage of GLBA's privacy requirements.[44]

The privacy provisions of GLBA impose two other basic obligations on financial institutions. First, financial institutions are required to implement policies and procedures governing data access, security and integrity as may be required by the federal financial institutions regulatory agencies.[45] Second, Title V prohibits the obtaining of nonpublic personal information from

40. 15 U.S.C. § 6802(e) (Supp. V 1999).

41. 15 U.S.C. § 6802(b)(2) (Supp. V 1999).

42. 15 U.S.C. § 6802(d) (Supp. V 1999).

43. 15 U.S.C. § 6804(a)(1) (Supp. V 1999). Under the statute, these regulations were to have been adopted by November 13, 2000, the date on which Title V's requirements were to have become fully effective unless extended by agency regulatory action. *Id.* In June 2000, however, the federal financial institutions agencies adopted their final GLBA privacy regulations and made compliance with the new regulations mandatory as of July 1, 2001 (albeit "optional" as of November 13, 2000), citing in general the need to allow affected financial institutions sufficient time to bring themselves into compliance with the new requirements. Privacy of Consumer Financial Information, 65 Fed. Reg. 35, 162, 35,205 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.15).

44. According to the Conference Report that accompanied GLBA, the exclusion of CFTC-regulated entities, the Federal Agricultural Mortgage Corporation, entities chartered and operating under the Farm Credit Act of 1971, and organizations chartered and regulated under federal law that engage in secondary market or securitization transactions, was included because such entities "do not market products directly to consumers." H.R. CONF. REP. No. 106-434 (Nov. 1999) (accompanying H.R. 10).

45. 15 U.S.C. § 6804(a)(1) (Supp. V 1999).

financial institutions under false pretenses, which is referred to as the practice of so-called "pretext calling."[46] The federal financial regulatory agencies and state insurance regulatory authorities are each given the authority to implement and enforce the requirements of Title V with respect to financial institutions under their respective regulatory jurisdictions.[47] As discussed later in this article, the states have certain authority to enact privacy protections that are stricter than those provided under Federal law.[48]

Accordingly, GLBA Title V carries into effect most, if not all, of the "fair information" principles reflected in various public sector issuances and actions.[49] By requiring that financial institutions give their customers notice of their data collection, use, and disclosure policies and practices, GLBA implements the fair information principle of notice—the right of a consumer to be informed of a financial institution's information collection and use practices. The statute also carries out the fair information principle of *choice/consent* by giving financial institution customers certain specific rights to direct how their personal information can be used. Title V's requirements governing data access, security and integrity reflect the fair information principle of *integrity/security*, whereas the enforcement authority bestowed on the federal financial institution regulatory agencies and the state insurance authorities addresses the information principle of *enforcement/redress.* It is difficult to find in GLBA, however, any meaningful articulation of the fair information principle of *access/participation*, inasmuch as Title V simply does not address the rights of financial institution consumers to have consumer access to nonpublic personal information and the opportunity to correct it.

---

46. 15 U.S.C. § 6821(a) (Supp. V 1999).

47. 15 U.S.C. § 6805(a) (Supp. V 1999). Under Titles I and III of GLBA, the regulation of insurance activities of financial institutions is effectively left to state insurance regulatory authorities, subject to certain nondiscrimination requirements that are designed to ensure that financial institutions are not restricted or discriminated against in their conduct of insurance activities allowed under GLBA. 15 U.S.C. §§ 6701, 6711-6717 (Supp. V 1999).

48. *See infra* Part VI.B.2.

49. *See supra* text accompanying notes 20-27.

It is not sufficient simply to state that GLBA implements the principles of "fair information" without devoting at least some attention to how these principles are implemented. Notably, the rights of financial institution consumers to direct how their nonpublic personal information can be shared with others is limited to the right to *object* to such sharing with *third parties.* Consumers are not given the right to influence the sharing of information with financial institution *affiliates*, nor are they given the right to *affirmatively consent* to the sharing of personal data with non-affiliates. These legislative choices, as noted above, were intentional, and went to the heart of the "privacy compromise" that was reached in the fall of 1999.

In other contexts, notably HIPAA in the case of personal *medical* information and COPPA in the case of children's online information, Congress has made different choices. Under HIPAA, which governs personal medical information maintained through electronic media, a health care provider, insurer or business partner must obtain the affirmative consent of the individual prior to sharing personal information with a third party.[50] In the case of children's personal online information, the fair information *choice/consent* principle is implemented through the requirement that a children's web site operator obtain *verifiable parental consent* prior to collecting, using or sharing children's personal information.[51] Indeed, the relatively mild notice/consent provisions of GLBA Title V were not universally applauded, and privacy advocates inside and outside of Congress have promised to revisit these choices in the future.

50. *Compare* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (to be codified at 16 C.F.R. pt. 313), *with* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,811-13 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 164).

51. 15 U.S.C. § 6502(b)(1)(A)(ii) (Supp. V 1999). *Compare* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646, 33,677 (May 24, 2000) (to be codified at 16 C.F.R. 313), *with* 15 U.S.C. § 6502(b)(1)(A)(ii) (Supp. V 1999).

V. GRAMM-LEACH-BLILEY PRIVACY REQUIREMENTS: SCOPE AND COVERAGE

A. "Financial Institution"

Title V applies to any entity that is a "financial institution" within the definition of GLBA. This definition, in turn, includes "any institution the business of which is engaging in financial activities" within the meaning of subsection 4(k) of the Bank Holding Company Act of 1956, (BCHA)[52] as amended by Title I of GLBA. This cross-reference is of no small significance, inasmuch as it refers to a key part of the new financial reform provisions of GLBA which were effectuated through changes to the BHCA, the federal law that regulates the ownership of banks by bank holding companies, and the nature and scope of their nonbanking activities. Those changes allow certain bank holding companies that satisfy specific capitalization, management and Community Reinvestment Act qualification criteria (so-called "good citizenship" conditions) to elect the status of "financial holding company" and engage in activities that are "financial" in nature, instead of being limited, as was the case under prior law, to activities that are "closely related to banking."[53] The definition of a "financial" activity, found in BHCA subsection 4(k), was drafted in a consciously broad manner in keeping with the congressional intent to expand in a material fashion the range of financial activities allowed for financial firms, and consequently captures a wide array of activities and business organizations.[54] The various federal regulations adopted under Title V confirm the potential broad scope of this Title by uniformly defining this provision to encompass an activity that is financial in nature or "incidental" to

52. 12 U.S.C. § 1843(k) (1994).

53. Section 4 of the BHCA generally restricts the ability of bank holding companies to engage in nonbanking activities. Under subsection 4(c)(8) of the BHCA, a bank holding company may acquire shares of a company that is engaged in an activity that is so "closely related to banking as to be proper incident thereto," as determined by the Federal Reserve Board. 12 U.S.C. § 1843(c)(8) (1994).

54. *See* H.R. CONF. REP. No. 106-434 (Nov. 1999) (accompanying H.R. 10).

a financial activity.[55] Most notable are the FTC regulations that define a financial institution as any entity that is "significantly engaged" in financial activities. The FTC regulations go on to list a variety of entities – including retail credit card issuers, personal property and real estate appraisers, check cashing businesses, tax preparation services and real estate settlement companies – to underscore the point.[56] Indeed, recent action by the Federal Reserve Board to propose including real estate brokerage as a "financial" activity under GLBA that can be conducted by financial holding companies[57] have been opposed by the real estate brokerage industry in part because such action would result in such persons being subject to GLBA's privacy requirements.[58]

B. "Consumers" and "Customers"

As noted above, two of Title V's major requirements consist of requiring financial institutions (1) to provide written notification to customers of their privacy policies, and (2) to give consumers the right to "opt out" of having their personal information shared with third parties. The language of Title V specifically applies the privacy policy requirements to financial institution "customers," and the "opt out" rights to financial institution "consumers."

This language has been applied literally by the financial institutions regulatory agencies in their implementing regulations. The regulations clarify, primarily through examples, the distinctions between "customers" and "consumers," stating that a "consumer" is an individual who obtains a financial product or

55. 65 Fed. Reg. 35,162, 35,197 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.3(k) for the OCC); 65 Fed. Reg. 35,162, 35,207 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.3(k) for the FRB); 65 Fed. Reg. 35,162, 35,220 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.6(k) for the FDIC); 65 Fed. Reg. 35,162, 35,227 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.3(k) for the OTS); 65 Fed. Reg. 40,334, 40,364 (June 29, 2000) (to be codified at 17 C.F.R. § 248(n)(1) for the SEC).

56. 65 Fed. Reg. 33,646, 33,678 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.3(k)).

57. 66 Fed. Reg. 307 (proposed Jan. 3, 2001).

58. *See, e.g.*, Press Release, National Association of Realtors, NAR Vows to Keep Banks Out Of Real Estate Brokerage (Jan. 22, 2001), http://nar.realtor.com/news/2001Releases/January/10.htm (last visited Mar. 1, 2001).

service from a financial institution that is to be used primarily for personal, family or household purposes,[59] whereas a "customer" of a financial institution is a consumer that has established a "continuing relationship" with a financial institution.[60] The net result of this distinction is that any individual that obtains any service from a financial institution, even in an isolated transaction such as a withdrawal from an automatic teller machine (ATM), is a "consumer" who is entitled to be told in advance if his personal information derived from that transaction will be shared with a third party. That consumer must be given the right to "opt out" of having that information shared, whereas a "customer" who is entitled to the right to receive the financial institution's written privacy notices must have a "continuing relationship" with the financial institution (generally in the form of an account or ongoing servicing relationship).

While, at first gloss, the application of Title V to an isolated ATM transaction by a consumer with a financial institution other than his or her bank may seem burdensome, in fact this legal consequence may be of more academic than practical concern,

---

59. 65 Fed. Reg. 35,162, 35,197 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.3(e) for the OCC)); 65 Fed. Reg. 35,162, 35,207 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.3(e) for the FRB); 65 Fed. Reg. 35,162, 35,220 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.6(e) for the FDIC); 65 Fed. Reg. 35,162, 35,227 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.3(e) for the OTS); 65 Fed. Reg. 40,334, 40,363 (June 29, 2000) (to be codified at 17 C.F.R. § 248(g)(1) for the SEC); 65 Fed. Reg. 33,646, 33,678 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.3(e) for the FTC). The use-based qualifier in the agency definitions essentially tracks the statutory definition and is consistent with the use of the term "consumer" in other financial consumer laws such as the Truth In Lending Act, 15 U.S.C. § 1602(h) (1994), the Truth In Savings Act, 12 U.S.C. § 4313 (1994), and the Electronic Funds Transfer Act, 15 U.S.C. § 1693(a)(5) (1994).

60. 65 Fed. Reg. 35,162, 35,197 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.3(f) for the OCC); 65 Fed. Reg. 35,162, 35,207 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.3(f) for the FRB); 65 Fed. Reg. 35,162, 35,220 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.6(f) for the FDIC); 65 Fed. Reg. 35,162, 35,227 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.3(f) for the OTS); 65 Fed. Reg. 40,334, 40,364 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248(j) for the SEC); 65 Fed. Reg. 33,646, 33,678 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.3(f) for the FTC). By way of illustration, the agency rules provide that a "continuing relationship" includes such transactions and relationships between and individual and a financial institution: a credit or investment account, purchase of an investment product from a financial institution, obtaining of financial, investment, economic, and tax advisory or counseling services from a financial institution, receipt of real estate settlement services, or ownership of loan servicing rights. *Id.*

inasmuch as the financial institution owner of the ATM can avoid having to provide any "opt out" notices and rights simply by not sharing the transaction information with a third party (other than as authorized pursuant to one of the nondisclosure exceptions, as more fully discussed below). By the same token, the limitation of consumer rights under GLBA to persons obtaining products and services primarily for *personal* use avoids the application of Title V to an individual's *commercial* activities (*e.g.,* a person's personal guarantee of a commercial loan), although this limitation may be of little comfort to a financial institution legal or compliance official charged with the obligation to design compliance or monitoring systems to distinguish between "consumer" and non-consumer transactions of an individual.

C. "Nonpublic Personal Information"

Title V's notice and "opt out" requirements apply only to the disclosure by a financial institution of "nonpublic personal information," a term that refers to "personally identifiable financial information" that is: (a) provided by a consumer to a financial institution, results from a transaction with or service performed for the consumer, or is otherwise obtained by the financial institution, *and* (b) is not "publicly available information" as defined by regulation.[61] The financial regulatory agencies wrestled with the concept of nonpublic personal information during their rulemaking proceedings, particularly with respect to when personal information was "publicly available." In the end, the agencies collectively included within the realm of publicly available information any information that a financial institution has a "reasonable basis" to believe is lawfully available to the general public from federal, state or local governmental records, widely distributed media (including the Internet), or disclosures to the general public required to be made by federal, state or local law. In turn, a financial institution has a "reasonable basis" if it takes steps to determine that the information is of a type generally available to the general public, and whether an individual can

61. 15 U.S.C. § 6809(4) (Supp. V 1999).

direct that such information not be so made available and, if so, the individual has not done so.[62] The latter clause, which is tied to the ability of an individual to control the disclosure of personal information, reflects the basic "fair information" principle of choice, namely, the principle that an individual should have the right to choose when personal information about him or her is disclosed.[63]

In this context, the effect of this regulatory definition is to exclude from the definition of "nonpublic personal information" consumer real estate and title records on file with governmental authorities, and telephone numbers *unless* the number is unlisted (the consumer has chosen not to allow that information to be publicly disclosed).[64] Under the statute and agency regulations, aggregate customer data on a list is not considered nonpublic personal information *unless* such data is derived from nonpublic personal information.[65]

62. 65 Fed. Reg. 35,162, 35,197 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.3(p) for the OCC); 65 Fed. Reg. 35,162, 35,207 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.3(p) for the FRB); 65 Fed. Reg. 35,162, 35,217 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.3(p) for the FDIC); 65 Fed. Reg. 35,162, 35,227 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.3(p) for the OTS); 65 Fed. Reg. 40,334, 40,365 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.3(v) for the SEC); 65 Fed. Reg. 33,646, 33,681 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.3(p) for the FTC).

63. *See supra* text accompanying note 25.

64. An alternative concept of "publicly available information" that was considered during the agency rulemaking process would have required a financial institution to have *actually obtained* that information from a public source. The financial agencies ultimately decided (to the relief of the financial services industry) on a more lenient standard that treated information as "publicly available" if a financial institution *could have* obtained it from a public source. *See* 65 Fed. Reg. 35,162, 35,171-72 (June 1, 2000).

65. 15 U.S.C. § 6809(4)(C) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,197 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.3(o)(2)(ii) for the OCC); 65 Fed. Reg. 35,162, 35,207 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.3(o)(2)(ii) for the FRB); 65 Fed. Reg. 35,162, 35,217 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.3(o)(2)(ii) for the FDIC); 65 Fed. Reg. 35,162, 35,227 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.3(o)(2)(ii)); 65 Fed. Reg. 40,334, 40,364-65 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.3(t)(3)(ii) for the SEC); 65 Fed. Reg. 33,646, 33,678 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.3(o)(2)(ii) for the FTC).

VI. GRAMM-LEACH-BLILEY PRIVACY REQUIREMENTS: NOTICE AND CHOICE

As noted above, at the heart of GLBA's privacy requirements are the privacy-based disclosure, notice and "opt out" provisions under which financial services consumers and customers have the right to be informed of a financial institution's privacy policies, as well as the right to direct a financial institution not to share nonpublic personal information with third parties.

A. Disclosure/Notice Requirements

Title V and the implementing agency regulations require financial institutions to provide customers with written notice of their privacy policies at the inception of the customer relationship, as well as on an annual basis.[66] The information required in initial and annual notices is substantially the same.

Privacy notices must be delivered (subject to certain exceptions) at the inception of a customer relationship.[67] They are *not* required to be given, however, to consumers (persons who obtain financial institution products and services without establishing a customer relationship) *if* the financial institution does not disclose any nonpublic personal information about the consumer to a third party.[68] In addition, the law and implementing regulations require the delivery of an annual privacy notice to customers (*i.e.*, at least once in any 12-month period that a customer relationship exists).[69] Again, the annual notice requirement is limited to financial institution customers, which, under the regulations, does not include *former* customers of the

66. 15 U.S.C. § 6803(a) (Supp. V 1999).

67. *Id.*

68. 15 U.S.C. § 6803(a), (b) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,199 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.4(a) for the OCC); 65 Fed. Reg. 35,162, 35,209 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.4(a) for the FRB); 65 Fed. Reg. 35,162, 35,219 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.4(a) for the FDIC); 65 Fed. Reg. 35,162, 35,229 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.4(a)) (OTS); 65 Fed. Reg. 40,334, 40,365 (June 29, 2000) (to be codified at 17 C.F.R. § 248.4(b) for the SEC); 65 Fed. Reg. 33,646, 33,681 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.4(a) for the FTC).

69. 15 U.S.C. § 6803(a) (Supp. V 1999).

financial institution.[70]

The regulations specify the form and content of the privacy notifications, as well as the manner of delivery. Generally, the information required to be included in the initial and annual privacy notifications includes: (1) the categories of nonpublic personal information collected and disclosed, (2) the categories of affiliates and third parties to which such information (including information about former customers) is disclosed, (3) any disclosure of information under joint marketing and similar arrangements, (4) an explanation of customer opt out rights, (5) information on any credit disclosures to affiliates made under the FCRA, and (6) the financial institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.[71] To the extent, however, that a financial institution discloses nonpublic personal information to third parties under one of the specific exceptions allowed under Title V, a financial institution need only disclose that it is disclosing information "as permitted by law."[72]

The regulations require that privacy notices must be "clear and conspicuous," which in turn is defined to mean that the notices

70. 15 U.S.C. § 6803(a) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,199 (June 1, 2000) (to be codified at 12 C.F.R. § 40.5 for the OCC); 65 Fed. Reg. 35,162, 35,210 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.5 for the FRB Board); 65 Fed. Reg. 35,162, 35,220 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.5 for the FDIC); 65 Fed. Reg. 35,162, 35,230 (June 1, 2000) (to be codified at 12 C.F.R. § 573.5 for the OTS); 65 Fed. Reg. 40,334, 40,366 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.5(b)(1) for the SEC); 65 Fed. Reg. 33,646, 33,682 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.5 for the FTC).

71. 15 U.S.C. § 6803(b) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,200 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.6 for the OCC); 65 Fed. Reg. 35,162, 35,210 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.6 for the FRB); 65 Fed. Reg. 35162, 35220 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.6 for the FDIC); 65 Fed. Reg. 35,162, 35,230 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.6 for the OTS); 65 Fed. Reg. 40,334, 40,366 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.6 for the SEC); 65 Fed. Reg. 33,646, 33,682 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.6 for the FTC).

72. 15 U.S.C. § 6803(b) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,200 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.6 for the OCC); 65 Fed. Reg. 35,162, 35,210 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.6 for the FRB); 65 Fed. Reg. 35162, 35220 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.6 for the FDIC); 65 Fed. Reg. 35,162, 35,230 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.6 for the OTS); 65 Fed. Reg. 40,334, 40,366 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.6 for the SEC); 65 Fed. Reg. 33,646, 33,682 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.6 for the FTC).

must be "reasonably understandable" and "designed to call attention" to the nature and significance of the information in the notice.[73] The general standard for the delivery of privacy notices is that they must be delivered in such a manner that the customer "can reasonably be expected to receive actual notice in writing" or, *if the customer agrees*, electronically (in the latter instance, subject to certain formatting requirements).[74]

To the extent a financial institution changes its policies and procedures with respect to the disclosure of nonpublic personal information, the financial institution must deliver a revised privacy notice to customers describing any relevant changes prior to disclosing such information.[75] This requirement does not extend to disclosures of nonpublic personal information to a new category of third party *if* the financial institution adequately disclosed such disclosure (or, more precisely, the possibility thereof) in a prior

73. 15 U.S.C. § 6803(a) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,197 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.3(b) for the OCC); 65 Fed. Reg. 35,162, 35,207 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.3(b) for the FRB); 65 Fed. Reg. 35,162, 35,217 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.3(b) for the FDIC); 65 Fed. Reg. 35,162, 35,227 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.3(b) for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.7 for the SEC); 65 Fed. Reg. 33646, 33678 (May 24, 2000) (to be codified at 16 C.F.R. pts. 313.3(b) (FTC).

74. 65 Fed. Reg. 35,162, 35,202 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.9 for the OCC); 65 Fed. Reg. 35,162, 35,212 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.9 for the FRB); 65 Fed. Reg. 35,162, 35,222 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.9 for the FDIC); 65 Fed. Reg. 35,162, 35,232 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.9 for the OTS); 65 Fed. Reg. 40,334, 40,368 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.9 for the SEC); 65 Fed. Reg. 33,646, 33,684 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.9 for the FTC). The "customer agreement" requirement for electronically-delivered notices are broadly consistent, in relevant part, with general requirements for delivery of consumer information by private and public enterprises under the Electronic Signatures in Global and National Commerce Act of 2000 ("E-Sign"), which became effective October 1, 2000. Act of June 30, 2000, Pub. L. 106-229, 114 Stat. 464 (2000). E-Sign broadly codifies under federal law the validity of electronic signatures in commerce, but contains a number of requirements specifically governing the use of electronic media with consumers, consumer disclosure, consent, operability and "technology neutrality" requirements. E-Sign § 102(c), 15 U.S.C.A. § 7002 (West Supp. 2000).

75. 65 Fed. Reg. 35,162, 35,202 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.8 for the OCC); 65 Fed. Reg. 35,162, 35,212 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.8 for the FRB); 65 Fed. Reg. 35,162, 35,222 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.8 for the FDIC); 65 Fed. Reg. 35,162, 35,232 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.8 for the OTS); 65 Fed. Reg. 40,334, 40,368 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.8 for the SEC); 65 Fed. Reg. 33,646, 33,684 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.8 for the FTC).

notice. Thus, financial institutions may anticipate the future disclosure of new categories of nonpublic personal information to new classes of third parties in their privacy notices.[76]

B. Notice/Opt-Out Requirements

The fair information principle of consumer choice is implemented in Title V by its notice and opt-out provisions, under which a financial institution must provide written notice to financial institution consumers of its policies and practices governing the disclosure of nonpublic personal information to affiliates and third parties, and provide consumers the opportunity to opt out of the disclosure of their nonpublic personal information with unaffiliated third parties.[77] Title V, however, contains a number of exceptions to the notice/opt-out requirements that generally allow financial institutions to share nonpublic personal information with certain types of third parties (*e.g.*, servicing providers, credit card affinity partners, law enforcement agencies, rating agencies, the financial institution's attorneys and accountants, consumer reporting agencies under the FCRA, and other specified persons) and for specific types of transactions and activities (*e.g.*, for account servicing or processing transactions, to provide reports on account transactions, to protect against or prevent fraud, in securitization or business combination transactions, in connection with account sales or audit activities, or as otherwise required by law).[78]

---

76. 65 Fed. Reg. 35,162, 35,202 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.8 for the OCC); 65 Fed. Reg. 35,162, 35,212 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.8 for the FRB); 65 Fed. Reg. 35,162, 35,222 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.8 for the FDIC); 65 Fed. Reg. 35,162, 35,232 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.8 for the OTS); 65 Fed. Reg. 40,334, 40,368 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.8 for the SEC); 65 Fed. Reg. 33,646, 33,684 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.8 for the FTC).

77. 12 U.S.C. § 6802 (Supp. V 1999).

78. 15 U.S.C. § 6802(e) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,204 (June 1, 2000) (to be codified at 12 C.F.R. pts. 40.13-15 for the OCC); 65 Fed. Reg. 35,162, 35,214-15 (June 1, 2000) (to be codified at 12 C.F.R. pts. 216.13-15 for the FRB); 65 Fed. Reg. 35,162, 35,224, 35,225 (to be codified at 12 C.F.R. pts. 332.13-15 for the FDIC); 65 Fed. Reg. 35,162, 35,234 (June 1, 2000) (to be codified at 12 C.F.R. pts. 573.13-15 for the OTS); 65 Fed. Reg. 40,334, 40,370-71 (June 29, 2000) (to be codified at 17 C.F.R. pts. 248.13-15, for the SEC); 65 Fed. Reg. 33,646, 33,686-87 (May 24, 2000) (to be codified at 16 C.F.R. pts. 313.13-15 for the FTC).

Of the various exceptions to the notice/opt out provisions, the servicing exception, which broadly allows financial institutions to share nonpublic personal information with nonaffiliates "as necessary to effect, administer or enforce a transaction that a consumer authorizes or requests" or in connection with servicing, processing or maintaining a consumer account or transaction, is probably of most practical significance, at least from the standpoint of enabling financial institutions to process or service account transactions without having to give their customers notice and opt-out rights. Moreover, a financial institution's disclosure of nonpublic personal information under these various exceptions need not be specifically disclosed to financial institution consumers; it suffices, for purposes of compliance with Title V regulations, that consumers and customers be informed merely that nonpublic personal information can be disclosed to third parties "as permitted by law." This latter feature also allows financial institutions that do not intend to disclose nonpublic personal information other than pursuant to one of the transactional exceptions to use a "short-form" privacy notification in making required Title V disclosures to consumers and customers.

Title V and the regulations also allow a financial institution to disclose, without providing an opt-out notice and opt-out rights, nonpublic personal information to a third party who is performing services for, or functions on behalf of, the financial institution, including marketing services, provided that certain conditions are met.[79] In general, the financial institution must enter into a written contract with the third party that, among other things, prohibits the third party from disclosing or using the nonpublic personal information other than for the purposes for which such information was provided, or under one of the specified disclosure exceptions in the statute and regulations, and must provide an initial privacy notice. The agreement in question also can consist of a joint marketing agreement between two or more financial institutions. Financial institution customers, however, must be separately informed in the financial institution's privacy notices

79. 15 U.S.C § 6802(b)(1)(C)(2) (Supp. V 1999).

that nonpublic personal information may be disclosed in this manner.

The opt-out rights under Title V and the regulations are relatively straightforward in concept: a consumer must be given notice and a "reasonable opportunity" to opt out of having his or her nonpublic personal information disclosed to a third party *prior to such disclosure.*[80] The requirement of reasonable opportunity can be fulfilled by a variety of means (including mail or electronic means if the consumer agrees), but generally contemplates that the consumer may have up to thirty days to make his or her opt out election.[81] The consumer also may elect to exercise a partial opt out, directing that certain nonpublic personal information not be shared with third parties while allowing other types of nonpublic personal information to be shared. A consumer's opt-out election must be honored by the financial institution as "soon as reasonably practicable" after the financial institution receives it. Further, the opt-out is effective until revoked by later action of the consumer, and a consumer may elect to exercise his or her opt-out rights at any time.[82]

---

80. 15 U.S.C. § 6802 (a),(b) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,201-02 (June 1, 2000) (to be codified at 12 C.F.R. pts. 40.7, .10 for the OCC); 65 Fed. Reg. 35,162, 35,211-13 (June 1, 2000) (to be codified at 12 C.F.R. pts. 216.7, ..10 for the FRB); 65 Fed. Reg. 35,162, 35,221, 35,223 (June 1, 2000) (to be codified at 12 C.F.R. pts. 332.7, .10 for the FDIC); 65 Fed. Reg. 35,162, 35,231, 35,233 (June 1, 2000) (to be codified at 12 C.F.R. pts. 573.7, .10 for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified at 17 C.F.R. pts. 248.7, .10 for the SEC); 65 Fed. Reg. 33,646, 33,683-85 (May 24, 2000) (to be codified at 16 C.F.R. pts. 313.7, .10 for the FTC).

81. Moreover, the consumer cannot be required to write a letter in order to exercise his or her opt out rights. 65 Fed. Reg. 35,162, 35,201 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.7(a)(2) for the OCC); 65 Fed. Reg. 35,162, 35,215 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.17(a)(2) for the FRB); 65 Fed. Reg. 35,162, 35,221 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.7(a)(2) for the FDIC); 65 Fed. Reg. 35,162, 35,231 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.7(a)(2) for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.7(a)(2) for the SEC); 65 Fed. Reg. 33646, 33683 (to be codified at 16 C.F.R. pt. 313.7(a)(2) for the FTC).

82. 65 Fed. Reg. 35,162, 35,201 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.7(e), (f) and (g) for the OCC); 65 Fed. Reg. 35,162, 35,215 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.17(e), (f) and (g) for the FRB); 65 Fed. Reg. 35,162, 35,221 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.7(e), (f) and (g) for the FDIC); 65 Fed. Reg. 35,162, 35,231 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.7(e), (f) and (g) for the OTS); 65 Fed. Reg. 40,334, 40,368 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.7(e), (f) and (g) for the SEC); 65 Fed. Reg. 33,646, 33,683 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.7(e), (f) and (g) for the FTC).

In the case of a financial institution's transactions with a consumer that are isolated in nature (*e.g.*, an ATM transaction), the financial institution can simply give the consumer an opt-out notice and ask that the consumer decide, as part of the transaction, whether to opt out before completing the transaction. The notice/opt out rights, however, extend to former customers of the financial institution, so that a financial institution must ensure that nonpublic personal information concerning former customers is maintained and protected to the same extent as information concerning current customers. These rights also extend to joint accounts, although the agencies allow financial institutions some latitude in determining how to allow joint account holders to exercise their opt-out rights, *provided* that the financial institution explains in its opt-out notice how, and in what manner, joint account holders may exercise their opt-out rights.[83]

Title V and the implementing regulations address the knotty question of redisclosure of nonpublic personal information by a recipient thereof. While the rules governing redisclosures are somewhat technical, the basic principle that applies across the board is that of "stand in the shoes." In other words, a recipient of nonpublic personal information from a financial institution or other person generally must maintain the confidentiality of such information and may redisclose the information to another third party only to the same extent as the party that provided the nonpublic personal information to that person.[84] This principle is true both with respect to recipients of nonpublic personal

83. 65 Fed. Reg. 35,162, 35,201 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.7(d) for the OCC); 65 Fed. Reg. 35,162, 35,215 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.17(d) for the FRB); 65 Fed. Reg. 35,162, 35,221 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.7(d) for the FDIC); 65 Fed. Reg. 35,162, 35,231 (to be codified at 12 C.F.R. pt. 573.7(d) for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.7(d) for the SEC); 65 Fed. Reg. 33,646, 33,683 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.7(d) for the FTC).

84. 15 U.S.C. § 6802(c) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,203 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.11 for the OCC); 65 Fed. Reg. 35,162, 35,213 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.11 for the FRB); 65 Fed. Reg. 35,162, 35,223 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.11 for the FDIC); 65 Fed. Reg. 35,162, 35,233 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.11 for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.11 for the SEC); 65 Fed. Reg. 33,646, 33,685 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.11 for the FTC).

information under one of the transactional exceptions, as well as to the service provider/joint marketing exception. It does mean, however, that a recipient of nonpublic personal information can redisclose that information to its own affiliates – although those affiliates in turn are subject to the same restrictions on use and redisclosure – as well as to affiliates of the financial institution from which the nonpublic personal information was received.[85]

C. *Marketing Disclosure Prohibitions*

GLBA and the implementing privacy regulations contain separate prohibitions on the disclosure of account identifying information to third parties for marketing purposes, including telemarketing, direct mail marketing and electronic marketing.[86] These separate prohibitions directly address the unauthorized sale of customer account information to telemarketers and similar entities, a practice that has been of particular concern to federal and state authorities alike. The prohibition extends to disclosure of an account number or similar form of access number or code for a consumer credit card, deposit or transaction account to an unaffiliated third party, other than a consumer reporting agency within the meaning of the FCRA. Interestingly, these prohibitions do not seem to contemplate any form of customer consent to account identifier disclosures to marketers.

The agencies, in their implementing regulations, have added some detail to the framework and mechanics of this prohibition that are not directly reflected in the law itself.[87] Thus,

85. 15 U.S.C. § 6802(c) (Supp. V 1999); 65 Fed. Reg. 35,162, 35,203 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.11 for the OCC); 65 Fed. Reg. 35,162, 35,213 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.11 for the FRB); 65 Fed. Reg. 35,162, 35,223 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.11 for the FDIC); 65 Fed. Reg. 35,162, 35,233 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.11 for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified at 17 C.F.R. pt. 248.11 for the SEC); 65 Fed. Reg. 33,646, 33,685 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.11 for the FTC).

86. 15 U.S.C. § 6802(d) (Supp. V 1999).

87. 65 Fed. Reg. 35,162, 35,203 (June 1, 2000) (to be codified at 12 C.F.R. pt. 40.11 for the OCC); 65 Fed. Reg. 35,162, 35,213 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.11 for the FRB); 65 Fed. Reg. 35,162, 35,223 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.11 for the FDIC); 65 Fed. Reg. 35,162, 35,233 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.11 for the OTS); 65 Fed. Reg. 40,334, 40,369 (June 29, 2000) (to be codified

the agency rules exclude *encrypted* account numbers from the definition of account number provided that the recipient does not have the means to decode the number.[88] Further, the rules allow a financial institution to disclose account identifier information to its own agent or service provider solely for purposes of marketing the financial institution's own products or services (*provided* the agent or servicer cannot initiate direct charges to the account), as well as to a private label or affinity card or program participant that was identified to the customer when he or she entered the program.[89]

D. Administration and Enforcement; Other Liability

One of the core principles reflected in GLBA is that of "functional regulation," which refers to the proposition that the different activities of a financial services firm each should be regulated by the governmental authority with jurisdiction over that activity. GLBA, among other things, gave banking organizations the authority to conduct general securities and insurance activities, but specifically gave the regulatory authorities that historically had jurisdiction over those activities the authority to regulate them in the banking organization. Thus, the SEC was given the authority to regulate securities brokerage and dealing activities of banking organizations,[90] while state insurance regulators were given the

---

at 17 C.F.R. pt. 248.11 for the SEC); 65 Fed. Reg. 33,646, 33,685 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.11 for the FTC).

88. 65 Fed. Reg. 35,162, 35,204 (June 1, 2000) (to be codified at 12 C.F.R. § 40.12(c)(1) for the OCC); 65 Fed. Reg. 35,162, 35,214 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.12(c)(1) for the FRB); 65 Fed. Reg. 35,162, 35,224 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.12(c)(1) for the FDIC); 65 Fed. Reg. 35,162, 35,234 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.12(c)(1) for the OTS); 65 Fed. Reg. 40,334, 40,370 (June 1, 2000) (to be codified at 17 C.F.R. pt. 248.12(c)(1) for the SEC); 65 Fed. Reg. 33,646, 33,686 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.12(c)(1) for the FTC).

89. 65 Fed. Reg. 35,162, 35,204 (June 1, 2000) (to be codified at 12 C.F.R. § 40.12(b)(2) for the OCC); 65 Fed. Reg. 35,162, 35,214 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216.12(b)(2) for the FRB); 65 Fed. Reg. 35,162, 35,224 (June 1, 2000) (to be codified at 12 C.F.R. pt. 332.12(b)(2) for the FDIC); 65 Fed. Reg. 35,162, 35,234 (June 1, 2000) (to be codified at 12 C.F.R. pt. 573.12(b)(2) for the OTS); 65 Fed. Reg. 40,334, 40,370 (June 1, 2000) (to be codified at 17 C.F.R. pt. 248.12(b)(2) for the SEC); 65 Fed. Reg. 33,646, 33,686 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313.12(b)(2) for the FTC).

90. *See* Gramm-Leach-Bliley Act § 201-241, which amends several of the federal securities laws to enhance the regulatory jurisdiction of the SEC over various bank securities activities.

right to regulate (subject to certain nondiscrimination and other conditions) banking organizations' insurance activities.[91] The SEC is therefore the "functional regulator" of financial institution securities activities, and the state insurance authorities are the "functional regulators" of financial institution insurance activities.

This principle has been carried over squarely into the administration and enforcement provisions of Title V in that each of the five financial institutions regulatory agencies, the SEC, and the various state insurance regulatory authorities have been charged with implementing the GLBA privacy requirements for their respective "functional regulation" constituents.[92] In addition, for all entities that engage in financial activities but otherwise are not regulated by the banking, securities or insurance regulatory authorities, the FTC becomes the "catch-all" privacy regulator of those entities.

The allocation of privacy responsibilities among various federal and state agencies in this fashion is fully consistent with the overall thrust of GLBA, and also is consistent with historical divisions of regulatory authority under the various laws administered and enforced by these various bodies. At the same time, the proliferation of privacy regulators in principle poses a challenge to diversified financial services organizations that are engaged in a broad array of financial activities. Indeed, there are a number of financial firms that, as of July 1, 2000 will, through their various subsidiary organizations, become subject to the privacy regulations of several federal and/or state regulators. To forestall the possibility of inconsistent privacy regulations, GLBA does direct the financial privacy regulators to consult and coordinate among themselves in adopting regulations that, "to the extent

91. *See* Gramm-Leach-Bliley Act, §104, §§ 301-316.

92. Hence, under Title V the OCC becomes the privacy regulator for national banks, the Federal Reserve Board for state member banks and bank/financial holding companies, the FDIC for state nonmember banks, the OTS for savings institutions, the NCUA for credit unions, the SEC for regulated securities firms (broker-dealers, investment advisers and investment companies), and the state insurance commissions for insurance underwriters and agencies. In the relatively limited instances of banks conducting certain limited forms of insurance agency activities, (*e.g.*, title insurance), however, the banks' principal federal financial regulators will continue to oversee the privacy responsibilities of their respective constituents.

possible," are consistent and comparable among themselves.[93] Fortunately, the final regulations adopted by the interested agencies appear in the main to accomplish this important objective.

Similarly, the responsibility for the enforcement of Title V is allocated in the same manner among the various federal and state financial regulators, and the FTC. Each of the various regulators, in turn, may enforce Title V and the implementing regulations though the exercise of their respective administrative enforcement authorities.

Title V appears to confer no private right of action on aggrieved consumers, and consumers in turn will have to pursue such legal remedies as may otherwise be available to them under existing law (*e.g.*, state consumer protection statutes) without the benefit of additional authority under Title V. This absence of an express right of action, however, should not lull financial institutions into believing that they are shielded from private liability for noncompliance with federal (or state) privacy requirements. The possibility of private actions based on inadequate privacy practices is very real, inasmuch as inadequate or noncompliant practices may well give rise to liability under federal or state consumer protection statutes. In fact, the possibility of privacy-based call action litigation already has emerged,[94] and it does not strain the imagination to state that consumer protection litigation based on privacy rights could be fertile ground in the future for the plaintiffs' bar.

93. 15 U.S.C. § 6804(a)(2) (Supp. V 1999).

94. In the wake of the *U.S. Bancorp* state action, class action litigation was instituted against the respondent bank based on that action and alleging violations of state consumer protection laws. *See* Hatch v. U.S. Bank Nat'l Assoc., et al., No. 0:99cv872 (D. Minn. filed June 9, 1999), *available at* http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_06091999.html (last visited Mar. 1, 2001). The action was later settled (settlement details *available at* http://www.ag.state.mn.us/consumer/privacy/pr/pr%5Fusbank%5F07011999.html (last visited on Mar. 1, 2001)).

VII. GRAMM-LEACH-BLILEY PRIVACY REQUIREMENTS: INTERACTION WITH OTHER LAWS

As has been discussed above, the privacy protections of Title V have not been enacted in a vacuum. GLBA's provisions need to be understood and applied in the context of a variety of other laws and requirements arising at the federal and state levels. In certain respects, GLBA specifically addresses how the Title V provisions are to be construed in relation to other laws; on other respects, however, GLBA is silent as to the possible impact of other legal requirements. Conceptually, the operating principle for interpreting and applying Title V in light of other federal and state laws is one of the "highest common denominator;" namely, to the extent that there are inconsistencies between the requirements of GLBA on the one hand, and other federal or state law on the other hand, the more stringent legal requirements will prevail. This can be demonstrated by a brief examination of the interplay.

A. Interplay with Federal Laws

1. Fair Credit Reporting Act (FCRA)

The FCRA broadly regulates the collection, use, and disclosure of consumer credit information in consumers' personal transactions with credit providers, in particular the collection and use of such information by consumer reporting agencies. As a general matter, entities that fall into the definition of a "consumer reporting agency" are subject to a number of specific requirements governing the collection, use and disclosure of consumer credit information, including obligations to provide consumers with the opportunity to access and correct such information, strict limitations on the disclosure of consumer credit information, and substantial penalties for noncompliance.

Under the FCRA, a creditor that discloses "consumer report" information becomes a consumer reporting agency and

therefore is subject to the extensive FCRA requirements applicable to such entities. In 1996, Congress amended the FCRA to provide, among other things, that a "consumer report" does not include the communication of consumer credit information (excluding consumer transaction and experience information, which is not subject to disclosure restrictions) to affiliated persons, provided that the creditor "clearly and conspicuously" discloses to the consumer that such information may be communicated among such persons, *and* the consumer is given the opportunity to "opt out" of such disclosures.[95] These same amendments, however, prohibited the FTC and the financial institutions agencies from adopting implementing regulations with respect to this provision.[96]

GLBA amended the above-referenced provisions of the FCRA to repeal the rulemaking prohibition and direct the agencies to prescribe joint regulations as necessary to carry out the purposes of the FCRA. GLBA, however, also provides that it shall not be construed to "modify, limit or supercede the operation of the [FCRA]."[97] In this fashion, GLBA has added *additional* FCRA notice and opt-out requirements under Title V, including requirements for financial institutions to include in their initial and annual privacy notifications any disclosures of affiliate sharing and opt out rights required to be provided under the FCRA.[98] At the same time, the clear intent of GLBA is not to disturb the applicability of FCRA's other requirements.

The interplay of the general GLBA privacy requirements on the one hand, and the FCRA on the other hand, may create some difficulties in implementation. In proposed regulations to implement the FCRA provisions of Title V,[99] the agencies noted that their intention was to conform the financial institution privacy requirements under Title V with the specific requirements under the FCRA, such as proposed requirements governing the form and

95. 15 U.S.C. §1681a(d)(2) (Supp. V 1999) (*added by* Pub. L. 104-208, 110 Stat. 3009 (1996)).

96. 15 U.S.C. § 1681s(a)(4) (1994).

97. 15 U.S.C. § 6806 (Supp. V 1999).

98. 15 U.S.C. § 6803(b)(4) (Supp. V 1999).

99. *See* Proposed Rules for Fair Credit Reporting Regulations, 65 Fed. Reg. 63,120 (proposed Oct. 20, 2000) (issued by the OCC, OTS, Federal Reserve Board and FDIC).

content of opt-out notices and requirements that are consistent with the corresponding requirements under the GLBA privacy regulations. In fact, however, there is the possibility that the agencies' final FCRA regulations may depart in some respects from the requirements of the agencies' general financial institution privacy regulations.[100] The possibility of such inconsistencies has elicited criticism from the financial services industry which is concerned about the practical difficulties in preparing the requisite notices prior to July 1, 2001 without the benefit of knowing what additional requirements, if any, may be adopted under the FCRA.

2. Other Federal Laws

The possibility that financial institutions may collect nonpublic personal information that is covered by another federal law means that financial institutions will need to be sensitive to the application of these other requirements as they comply with Title V's requirements. For instance, financial institutions may collect nonpublic personal information that contains medical information (*e.g.,* information collected in a consumer application for life insurance) that would be subject to the medical records disclosure restrictions of HIPAA and implementing HHS regulations, which depart in at least one critical respect from the requirement of Title V by requiring the *affirmative consent* of a consumer prior to disclosure to a third party.[101] The financial institutions agencies, in adopting their regulations under Title V, acknowledged that HIPAA might apply to nonpublic personal information collected by financial institutions, and specifically indicated that some such information may be subject to both the Title V and to HIPAA. The agencies indicated their intention to consult with HHS, after the adoption of final HIPAA rules by the latter, to avoid the

100. *See id.* For instance, the agencies have asked whether the FCRA opt-out notices should disclose how long a consumer has to exercise his or her opt-out rights as well as the fact that a consumer may opt out at any time - two disclosures not required under the general GLBA privacy regulations. *Id.*

101. *See, e.g.,* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,810-12 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 164.506, .508).

imposition of duplicative or inconsistent requirements.[102] At the same time, it is quite clear that to the extent financial institutions collect nonpublic personal information that qualifies as medical information subject to HIPAA, the affirmative consent requirements for the disclosure of such information to third parties presumptively will apply.

The same result would seem to apply to financial institutions that operate web sites directed at or used by children under thirteen years of age, who, in turn, would be subject to the requirements of COPPA, including its requirement that "verifiable parental consent" be obtained prior to the collection of personal information about children.[103] Thus, where a financial institution proposes to collect nonpublic personal information relating to children via the Internet – a possibility that is becoming increasingly prevalent as financial institutions offer products and services online – the affirmative parental consent requirements of COPPA and implementing FTC regulations would be applicable, *in addition* to the general notice requirements of GLBA. The practical effect of this result, however, would be that COPPA would supercede the relatively more lenient requirements of Title V. At the same time, it remains to be seen whether the provisions of COPPA, which extend only to online children's information collection and use practices, will pose significant practical problems for financial institutions during implementation in conjunction with Title V.

In addition, the general Federal legislative interest in Internet privacy is leading to the introduction in Congress of legislation addressing this issue. At this time, however, how these legislative actions, if enacted into law, will affect Title V and its existing regulations remains to be seen, although the principle of "highest common denominator" (*i.e.,* that the most stringent legal requirement will apply) mentioned above is likely to prevail.

---

102. Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162, 35,164 (June 1, 2000).

103. *See supra* notes 16, 17.

B. Interplay with State Laws

The impact of GLBA privacy requirements on state law—and vice-versa—is an intriguing element of the new financial privacy scheme. As noted above, in certain respects GLBA confers direct jurisdictional authority on state regulators, namely, insurance regulators that are charged with the implementation of Title V with respect to entities engaged in insurance activities subject to their regulation.[104] Title V, however, contains a *partial* federal preemption of state law by providing that, subject to one important exception, to the extent (and only to the extent) of any inconsistency between Title V and any "statute, regulation, order or interpretation" in effect in any state, the requirements of Title V and implementing regulations shall prevail.[105] This exception provides that where a "statute, regulation, order or interpretation" of a state affords any person "greater protection" than that provided under Title V, *as determined by the FTC* (1) after consultation with the functional regulatory agency with jurisdiction over either the person that initiates or is the subject of the complaint, (2) on its own motion, or (3) upon petition of any interested party, such state action shall not be deemed inconsistent with Title V.[106] In other words, Title V will allow state authorities of any kind, by order or interpretation, to adopt (with FTC concurrence) financial privacy requirements that are more stringent than the protections created under GLBA.

The full impact of this partial preemption scheme remains to be seen, but there is no question that the authority reserved to the states to "out-tough" the federal regulators under Title V opens the door to state action across the country that, in turn, could seriously complicate the privacy compliance obligations of financial institutions doing business in multiple states. The likelihood of state action, moreover, probably is increased by the fact that states need *not* enact legislation to override Title V.

104. This state regulatory process already is underway. *See, e.g.*, N.Y. Ins. Dept., Regulation 169, *Privacy of Consumer Financial and Health Information*, 11 N.Y.C.R.R. 420 (2000).

105. 15 U.S.C. § 6807(a) (Supp. V 1999).

106. 15 U.S.C. § 6807(b) (Supp. V 1999).

States can act by regulation, order or even interpretation in so doing.[107] While a state override does require a finding of the FTC in order to be legally effective, Title V appears to give the FTC little, if any, regulatory discretion in this task. At the same time, the conferral on the FTC of this quasi-adjudicatory authority certainly enhances the FTC's regulatory authority under federal privacy law over financial institutions' privacy-related activities, particularly insofar as the FTC has the authority to make a state preemption determination *on its own motion.*

Hence, GLBA, in effect, creates an uneasy coexistence between federal and state financial privacy laws. Although the federal scheme in the ordinary course will dictate the financial privacy obligations of financial institutions, the states can act to impose different and more stringent regulatory requirements, and these requirements need not be consistent as among the several states. It is for this reason that the financial services industry has urged Congress to revisit the federal/state law interaction under Title V and reduce the authority of the states to adopt inconsistent requirements, a measure that understandably is opposed by the states and their legislative representatives.

Notwithstanding the partial preemption provisions of Title V, there remains the ever-present possibility of state actions based on existing consumer protection laws, which the states and private litigants undoubtedly will continue to bring. What is less certain, however, is the extent to which such state laws can, or should, be preempted under Title V, although one can fairly expect the states to argue that federal law should not override state consumer protection laws of a general nature, even where they are invoked to enforce consumer financial privacy rights. Neither GLBA nor the regulations address this issue, which presumably will have to await future action to be answered.

107. Thus, the outer boundaries of this state override authority might even extend to actions such as opinions of state attorneys general.

VIII. SECURITY AND INTEGRITY OF CUSTOMER DATA; FRAUDULENT INFORMATION-COLLECTION PRACTICES

Less prominent, though still significant, provisions of Title V are two additional series of requirements that: (1) address the security and integrity of nonpublic personal information, and (2) prohibit certain information-collection practices that are fraudulent in nature, in particular "pretext-calling" practices. These two requirements, in effect, implement the fair information principle of integrity and security of nonpublic personal financial information discussed above.

With respect to confidentiality and security of customer data, § 501(b) of GLBA obliges the financial institutions regulatory agencies (and the FTC) to establish standards for financial institutions subject to their respective jurisdiction relating to administrative, technical and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in "substantial harm or inconvenience to any customer."[108] Title V also directs the federal banking agencies to impose such standards as "safety and soundness" standards within the meaning of section 39 of the Federal Deposit Insurance Act[109] but directs the other financial institutions regulatory authorities (SEC, FTC and state insurance regulators) to impose such standards by rule.[110] As a practical matter, for enforcement and compliance purposes the distinctions between guidelines and rules made by this provision are probably modest given the broad authority of the federal banking regulators to take administrative actions for actions constituting, among other things, "unsafe and unsound" banking practices without the need

108. 15 U.S.C. § 6801(b) (Supp. IV 1998)

109. 12 U.S.C. § 1831p-1 (1994). This section of the FDIA directs the federal banking agencies to adopt regulations establishing prudential (or "safety and soundness") standards for financial institution operations, financial condition and activities. *Id.*

110. 15 U.S.C. § 6505(b) (Supp. IV 1998).

to allege the violation of any published rule or regulation.[111]

The federal banking agencies, in turn, have recently adopted regulations that implement the data security requirements of Title V.[112] These requirements are formulated as guidelines rather than specific rules and require financial institutions to adopt and implement policies and procedures governing collection, security and confidentiality of personal financial information, and specify standards that financial institutions must meet in creating such policies. The financial institutions agency guidelines, however, do not specify the precise form and content of these policies and procedures, leaving the details of their creation and implementation to the financial institutions themselves. The financial institutions agencies, in turn, have indicated that they will assess the adequacy of required policies through the exercise of their examination and supervision powers. In addition, the FTC issued an advance notice of proposed rulemaking last fall seeking comment on the form and content of the rules it will adopt under the data security/integrity provisions of Title V.[113]

Subtitle B of Title V separately addresses the procurement of customer financial information through fraudulent means.[114] Subtitle B, among other things, imposes a flat prohibition on any person obtaining, attempting to obtain, or requesting another person to obtain or attempt to obtain customer information by "false pretenses," which is defined to include the making of false, fictitious or fraudulent statements or representations to any official or customer of a financial institution, or knowingly providing false documents to an officer, employee or agent of a financial institution.[115] This prohibition is subject to several enumerated exceptions dealing with activities of law enforcement

111. 12 U.S.C. § 1818(b) (1988).

112. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616 (Feb. 1, 2001) (to be codified at 12 C.F.R. pt. 30 for the OCC; 12 C.F.R. pts. 208, 211, 225, 263 for the FRB; 12 C.F.R. pts. 308, 364 for the FDIC; 12 C.F.R. pts. 568, 570 for the OTS).

113. Privacy of Consumer Financial Information – Security, 65 Fed. Reg. 54,186 (Sept. 7, 2000).

114. 15 U.S.C. §§ 6821-6827 (Supp. V 1999).

115. 15 U.S.C. § 6821 (Supp. V 1999).

agencies, insurance company fraud investigations authorized under applicable law, obtaining of information that is otherwise available as a public record under the federal securities laws, or activities of private investigators in connection with child support collection efforts. Subtitle B also provides for criminal penalties for "knowingly and intentionally" violating section 521, with enhanced penalties for aggravated cases.[116]

The administrative and enforcement scheme under Subtitle B is similar, but not identical, to that prescribed under the privacy requirements of Title V. In this regard, the federal banking agencies are given the authority to enforce Subtitle B with respect to depository institutions under their respective jurisdictional domains, but the FTC is given authority to enforce Subtitle B with respect to all other classes of financial institutions, with the same power and authority the FTC has under the Fair Debt Collection Practices Act (FDCPA)[117] to enforce compliance therewith.[118] The cross reference to the FDCPA means, among other things, that the FTC has at its disposal the full range of administrative authority available to it under the FTC Act, including the authority to act under its power to prevent or remedy unfair and deceptive practices under section five thereof.[119]

In addition, the federal financial institutions regulatory agencies are directed to review their regulations and guidelines applicable to financial institutions under their respective jurisdictions, and prescribe changes thereto as necessary to ensure that financial institutions have policies and procedures in place to prevent the unauthorized disclosure of customer information and to "deter and detect" activities prohibited under Subtitle B.[120] The agencies, however, are not otherwise required to adopt regulations under this Subtitle.

Finally, Subtitle B contains essentially the same scheme of partial federal preemption of inconsistent state law as is contained

116. 15 U.S.C. § 6823 (Supp. V 1999).
117. 15 U.S.C. §§ 1692 - 16920 (1994).
118. 15 U.S.C. § 6822 (Supp. V 1999).
119. 15 U.S.C. § 1692(l) (1994).
120. 15 U.S.C. § 6825 (Supp. V 1999).

in the general privacy requirements of Title V, discussed above.[121] Thus, under Subtitle B, state authorities are allowed to adopt, by "statute, regulation, order or interpretation," requirements that are more stringent than those adopted under Subtitle B as determined by the FTC.[122]

IX. LOOK AT THE FUTURE AND SOME CONCLUDING OBSERVATIONS

Although GLBA Title V and the implementing agency regulations represent the most current framework governing financial privacy rights at the federal, and to a significant extent the state, levels, this legal landscape will continue to change. First, among other things, a number of congressional representatives have indicated their dissatisfaction with the current privacy requirements under Title V, and have introduced, or plan to introduce, legislation that will augment the privacy rights of financial institutions' consumers and customers beyond those currently set forth in Title V and the agency regulations. Indeed, during the year 2000 (prior to the adjournment of the 106th session of Congress), over twenty-five bills were introduced by various members of Congress addressing financial privacy rights, in some cases creating more stringent requirements such as requiring financial institutions to obtain the affirmative consent of consumers before sharing their nonpersonal information with third parties.[123] Similar legislation is being introduced as the current session of Congress gets underway.[124] While none of the prior legislative initiatives were enacted into law in 2000, several of their sponsors have indicated their intention to reintroduce legislation in 2001.

In a related vein, numerous congressional initiatives to protect the privacy rights of individuals across the board have been

121. *See supra* text accompanying notes 104-106.

122. 15 U.S.C. § 6824 (Supp. V 1999).

123. *See, e.g.,* Financial Consumers' Bill of Rights Act, H.R. 4332, 106th Cong. (2000) (introduced on Apr. 14, 2000); Financial Information Privacy Protection Act of 2000, S. 2513, 106th Cong. (2000) (introduced on May 4, 2000).

124. *See, e.g.,* Financial Privacy Protection Act of 2000, S.30, 107th Cong. (2001) (introduced on Jan. 22, 2001 by Sen. Paul S. Sarbanes).

introduced in prior congressional sessions and undoubtedly will be reintroduced in the near future. These measures, which address, among other things, the use (or misuse) of social security numbers,[125] the establishment of a federal privacy commission to conduct a comprehensive study of privacy protection,[126] and other legislative measures addressing on-line and "medical financial privacy,"[127] have been and will continue to be topics of legislative discussion and debate. These actions, in turn, are likely to increase the pressure for additional financial services legislation with respect to the privacy rights of financial institutions' customers.

At the federal agency level, although the federal financial institutions regulatory agencies have already adopted their regulatory schemes under Title V, the possibility remains that additional regulations will be adopted as the agencies gain experience with the implementation of the new privacy requirements. For instance, as the HHS medical privacy regulations under HIPAA come into effect, the federal financial institutions agencies are expected to review and possible modify their regulations to ensure their consistency with HIPAA. In addition, however, the FTC, which by all accounts is becoming an increasingly important participant in the financial privacy regulatory landscape, can be expected to be assertive in the protection of privacy rights of consumers across the board, including those of consumers doing business with financial institutions under the FTC's purview. Moreover, the FTC will be asked to make determinations as to the interplay between state and federal privacy laws, particularly with regard to whether a specific state legislative or regulatory action is more stringent that its federal counterpart, and thus entitled to the state law preemption exception, discussed above, provided under section 507 of GLBA. [128] It also is worth mentioning that the Department

125. *See, e.g.,* Privacy and Identity Protection Act of 2000, H.R.4857, 106th Cong. (2000) (introduced on July 13, 2000); Amy Boyer's Law, S.2554, 106th Cong. (2000) (introduced on May 15, 2000).

126. *See,* Privacy Comm. Act, H.R. 4049, 106th Cong. (2000) (introduced on Mar. 21, 2000).

127. *See, e.g.,* Medical Financial Privacy Protection Act, H.R.4585, 106th Cong. (2000) (introduced on June 6, 2000).

128. This process already has begun. *See* Letter from Gary Preszler,

of the Treasury, in conjunction with the federal financial regulatory authorities and the FTC, is directed under GLBA to conduct a study of information-sharing practices among financial institutions and their affiliates and report back to Congress by January 1, 2002.[129] The contents of this report and accompanying recommendations may have an impact on the nature and direction of future legislative and regulatory initiatives in the privacy realm.

With respect to state action on financial privacy matters, many states have introduced privacy legislation and/or are expected to introduce such legislation in the near future. Undoubtedly, some of these state measures will be specifically designed to provide the more stringent protections that are permitted for states under Title V. Even in instances where states are not introducing legislation or regulations to override the federal protections of Title V, the various state insurance regulatory authorities will be adopting their Title V regulations as the "functional regulators" of financial institutions insurance activities under GLBA.

The potential impact of international action on privacy matters also cannot be ignored. Notwithstanding the current Safe Harbor Privacy Principles in effect with respect to data transfers from the EU to the United States,[130] (which, for the time being, do not cover personal financial data) it is likely that the EU will continue to pay attention to the protection of financial data of individuals within the EU member nations, and the potential applicability of the EU directive with respect to transfers of such data to, among other places, the United States. It is difficult to predict at this time what, if any, further developments may occur along these lines, but there is the distinct possibility that EU actions under its Privacy Directive will create additional pressures on the US legislative and regulatory authorities to enhance the privacy protections already conferred under GLBA.

Commissioner, State of North Dakota Department of Banking and Financial Institutions, to Robert Pitofsky, Chairman, FTC (Sept. 12, 2000), *at* http://www.ftc.gov/privacy/glbact/ndpetition.pdf (last visited Mar. 1, 2001) (requesting a section 507 determination that North Dakota's Disclosure of Customer Information law affords more protection than is provided under GLBA).

129. 15 U.S.C. § 6808 (Supp. V 1999).

130. *See supra* note 19.

Although it is not possible to predict the course of future privacy-related developments, one fact is now clear - the possibility that privacy protection will be left to the self-regulation efforts of the financial services industry is now gone. Variations of the basic "fair information" principles now have been applied to the financial services industry through compulsory legislative and regulatory requirements, and the possibility that this regulatory scheme may be "rolled back" ranges between slim and none.

One obvious result of this new regulatory scheme is the need for "financial institutions" of all kinds to develop the notices, disclosures, programs and policies necessary to bring themselves into compliance with Title V.[131] Although the conceptual requirements of the new law and the agency regulations are quite simple, the implementation and compliance tasks promise to be complex, especially for financial institutions that are large and/or engage in a wide variety of financial activities. For example, nonpublic personal information can reside in any number of locations and databases, and many institutions are finding, to their dismay, that even the task of cataloguing such information – to say nothing of the ways in which nonpublic personal information is used and/or disclosed – may be formidable. In order to ensure that the requisite level of organizational attention is brought to this important task, most institutions of any size are appointing persons (as "privacy officers" or similarly-titled job descriptions) with full-time responsibility for privacy implementation within their organizations. Still, all financial institutions must be mindful of the fact that compliance with these new requirements will be a "top to bottom" task for which the organization's directors and senior managers will be held legally accountable.

Thus, at the beginning of the new century, financial privacy now is comprehensively regulated at the federal level and, by all accounts, will be significantly regulated at the state level as well. What remains, therefore, is simply the continued development and refinement of this new privacy scheme, a process that will unfold over the coming months and years as the financial services

131. *See, e.g., Privacy Preparedness*, OCC Advisory Letter 2001-2, (Jan. 22, 2001), 2001 WL 83085; *Privacy Laws and Regulations – Summary of Requirements*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 67,651 (OCC Bulletin 2000-25, Sept. 8, 2000).

industry, its consumers and customers, and their respective regulatory and legislative bodies, gain increased knowledge and experience with financial privacy issues.